Domain 2:
Asset Security

CISSP Domain 2 Asset Security Detailed

Code:	CISSPD2ASDN
Version:	3
Date of version:	1/24/2019
Created by:	AL Nafi Content Writer
Approved by:	Nafi Content reviewers
Confidentiality level:	For members only

Change history

Date	Version	Created by	Description of change
2/1/2019	1	Nafi Edu Dept	AL Nafi mentors created the first set of notes.
2/10/2019	2	Nafi Edu Dept	AL Nafi mentors created the first set of notes.
4/24/2019	3	Nafi Edu Dept	AL Nafi mentors created the first set of notes.

Table of contents

1. Purpose, scope and users

The purpose of this document is to define CISSP domain for Nafi members Only. Please be honest to yourself and with Al Nafi and do not share this with anyone else. Everyone can join Al Nafi as we are so economical to begin with.

These notes covers all the key areas of Domain 2 and the notes are good until a new revision of CISSP syllabus comes from ISC2. Normally the cycle is around 3 years so since we had our last revision in 2018 June, the next update to the CISSP syllabus is expected around June 2021.

Please follow the following 5 step program if you want to master CISSP domain and pass the exam inshAllah.

1. Watch all the CISSP videos on the portal 8-10 times. Soak yourself with Brother Faisal words in what he is teaching and try to ask questions. Think like a Security Manager who does everything with due care and due diligence.
2. Read all the presentations is and the detailed notes at least 8-10 times. Pay attention to additional reading material recommended by Brother Faisal during his videos.
3. Practice all the flash cards multiple times on our website.
4. Practice all the MCQ's on our website. (Those who score 85% in 10 out of 15 tests [The last 10 sets are counted towards exam payment by Al Nafi] Al Nafi will pay their exam fee inshAllah. Please give dawah to 50 people to join Al Nafi if they want to study inshAllah)
5. Go for the CISSP exam once you are approved by Al Nafi and your examination fee is paid.

2. Asset Security

Asset Security within the context of the second domain of the CISSP® examination deals with the protection of valuable assets to an organization as those assets go through their lifecycle. Therefore, it addresses the creation/collection, identification and classification, protection, storage, usage, maintenance, disposition, retention/archiving, and defensible destruction of assets. To properly protect valuable assets, such as information, an organization requires the careful and proper implementation of ownership and classification processes, which can ensure that assets receive the level of protection based on their value to the organization. The enormous increase in the collection of personal information by organizations has resulted in a corresponding increase in the importance of privacy considerations, and privacy protection constitutes an important part of the asset security domain. Individual privacy protection in the context of asset security includes the concepts of asset owners and custodians, processors, remanence, and limitations on collection and storage of valuable assets such as information. This also includes the important issue of retention as it relates to legal and regulatory requirements to the organization. Appropriate security controls must be chosen to protect the asset as it goes through its lifecycle, keeping in mind the requirements of each of the lifecycle phases and the handling requirements throughout. Therefore, understanding and applying proper baselines, scoping and tailoring, standards selection, and proper controls need to be understood by the security professional. The asset security domain also addresses asset handling requirements and includes asset storage, labeling, and defensible destruction.

2.1. Assets, information and Other Valuable Resources

Any item deemed by a company to be valuable can be referred to as an asset. In other words, an asset is anything that has value to an organization. In many cases, assets are also referred to as resources. Both words, assets and resources, imply value to an organization and, therefore, must be protected based on the value that it represents to the organization. Value can be expressed in terms of quantitative and qualitative methodologies, and both of these valuation methods are used to determine the level of protection that the assets require. Qualitative asset valuation implies that value is expressed in terms of numbers, usually monetary value. It is often understood that expressing value of intangible assets, such as information, is very difficult and, in many cases impossible, to express in quantitative ways; therefore, value of intangible assets is usually expressed in terms of qualitative methodologies usually using grades such as “high,” “medium,” “low,” or other classification that can express the value of assets without using numbers. Understanding the actual value of assets becomes very important in understanding how to protect those assets because the value will always dictate the level of security required. It is important for us to understand that security is not always driven by risk but rather driven by value. In fact, if you think about it, what is risk anyway? Risk is something that can impact value, and therefore, to fully understand risk requires the full understanding of the value of the asset first. As we have just covered, an asset is an item of value to the organization. Value can be expressed in terms of quantitative (numbers/monetary) and qualitative (grades such as high/medium/low, or top secret/secret/ confidential, etc.). Examples of valuable assets include, and are not limited to, and in no particular order:

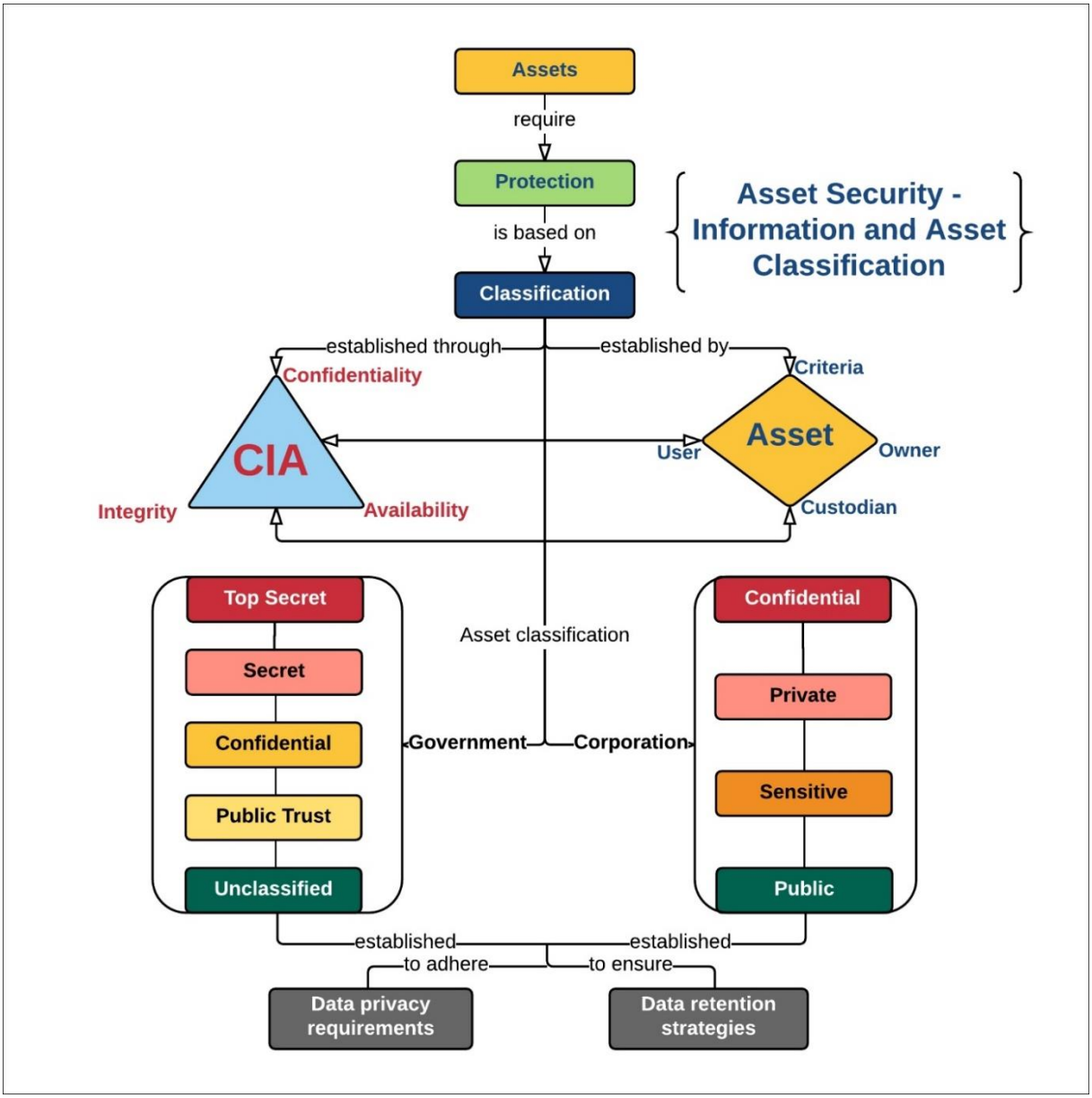
- People
- Information
- Data
- Hardware
- Software
- Systems
- Processes
- Devices
- Functions
- Ideas
- Intellectual property
- Corporate reputation
- Brand
- Identity
- Facilities

The list could include other assets, but the point has been made that any asset is really something that has value to an organization and requires careful protection based on that value. Therefore, protection will be dictated by the value. This domain, called Asset Security, deals with the methods to protect assets based on value.

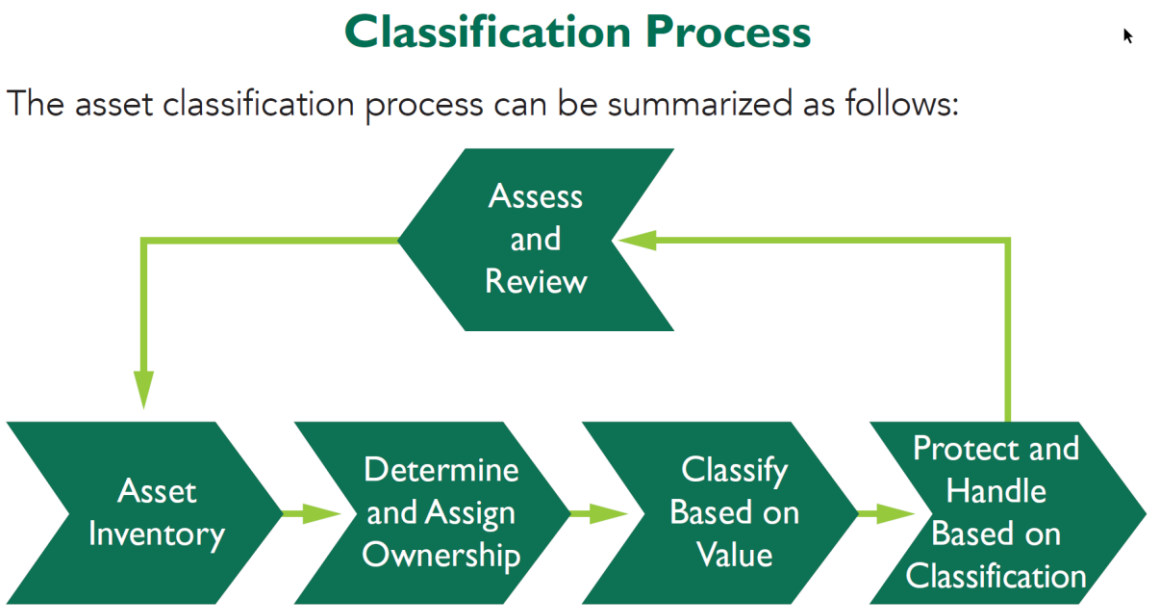
2.2. Identification/Discovery and Classification of Assets Based on Value

The value of assets will vary significantly, but to properly secure these assets, organizations need to identify and locate assets that may have value and then classify the assets based on value while defining how to properly protect each classification type. Assets, such as information, have become challenging to protect based on value. Organizations today are creating/collecting massive amounts of data, which makes discovery of this data for inventory purposes very difficult. To properly protect

assets, including information, organizations need to implement a formal asset classification system supported by proper management support, commitment, and conviction to ensure accountability. Proper policies need to be created and communicated to the entire organization to create the culture and set the tone for the effectiveness of the classification initiative. Organizations then need to understand fully where assets are created/used to establish an effective inventory system that will drive the classification process.



At this point, once assets have been located and identified, they can be classified by owners based on value and then protected based on classification. Classification of assets is essential to have proper controls be implemented to allow organizations to address compliance with relevant laws, regulations, standards, and policies. The first step in asset protection is to know what assets the organization has. In other words, an asset inventory is required before the organization can actually understand what assets they have that may have value.



Once we have an inventory of assets, understanding the value of those assets becomes the next step as it will drive asset classification, which, in turn, will drive the protection of those assets throughout their lifecycle. Having a complete inventory that is updated and reflective of creation/disposition/destruction of assets becomes very important. An updated and meaningful inventory of assets can then be used by the owners of those assets to determine value and classify assets based on that value.

The classification system will then determine the protection requirements.

2.3. Protection of the Value of Assets and Information

To better achieve goals and objectives, organizations today are generating massive amounts of information that obviously will represent organizational value. It is important for organizations to understand exactly the value that this information represents. Identifying and classifying assets and information will allow organizations to determine and achieve the protection requirements for the information.

These are the steps involved to do this properly:
1. Identify and locate assets, including information.
2. Classify based on value.
3. Protect based on classification.

The process of identifying assets that have value in the organization can be very challenging but nevertheless is a requirement to protect them accordingly. Valuable assets need to be identified in order to protect them accordingly. Assets can take many forms, here are a few examples:

Information assets
- Databases
- Files
- Spreadsheets
- Business continuity plans (BCPs)
- Procedures

Software

- Applications
- Source code
- Object code
- Operating systems

Physical assets

- Hardware
- Media
- Network equipment
- Servers
- Buildings

Processes and services

- Communications
- Data facilities
- Voice systems
- Computing

2.4. Classify Based on Value

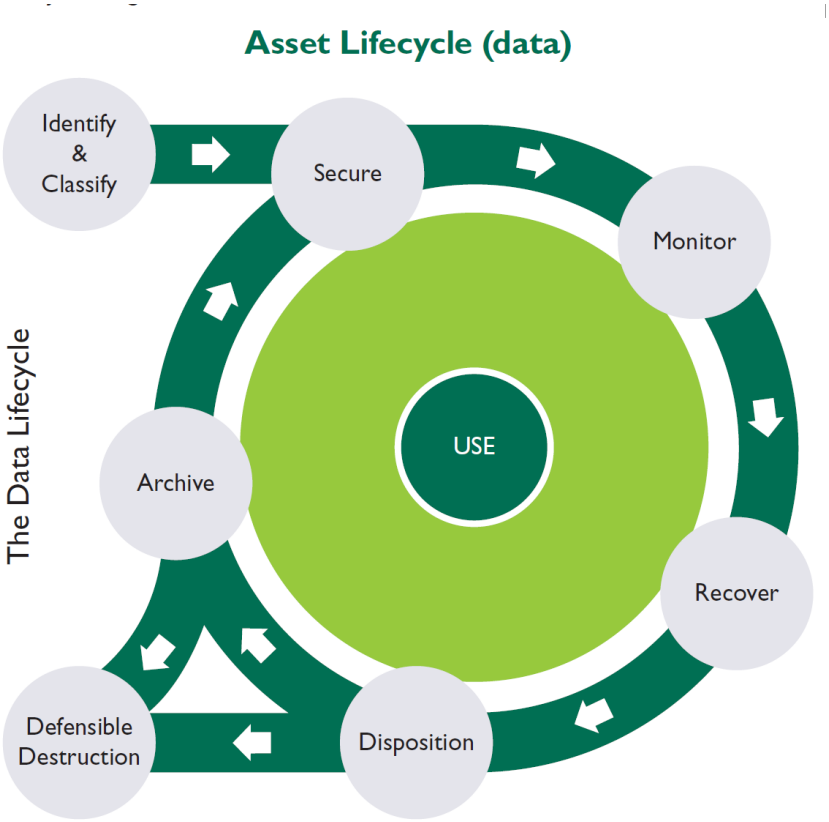
The next step in this process is to determine ownership to establish accountability. This may be easier for physical and tangible assets but the same needs to be done for intangible assets such as data. The owners are always in the best position to understand the value of what they own; therefore, it is up to the owners to classify assets. Determining value may not be easy. There are many factors and elements that need to be looked at to determine the true value of assets. For instance, we need to think about implications related to impact of disclosure, impact on corporate reputation, intellectual property, and trade secrets, etc. Regardless, the owner is always in the best position to truly understand the value of what they own to the organization. The process of understanding the value of an asset is very appropriately called asset valuation. The value of the asset will drive its classification level.

2.5. Protection Based on Classification

The next step in the classification process is to protect the assets based on their classification levels. A good way to achieve this would be to establish minimum security requirements for each of the classification levels that are being used. We refer to these as baselines. In other words, we can establish the minimum security baselines for each classification level that exists. Asset classification drives the security requirements that need to be implemented to protect the assets based on their value. Once the baselines have been determined, they can be applied to assets as they move through their lifecycle phases, including phases such as retention and destruction.

3. The Asset Lifecycle

To protect assets properly, one must understand the asset lifecycle and apply protection mechanism throughout the phases of the asset lifecycle. The protection will always be based on the value of those assets at particular points in the lifecycle phases. This implies that the parties accountable and responsible for the protection of assets must understand and monitor the value of assets as they go through their lifecycle. Those in the best position to do this are the owners of those assets, or designates of the owners.



Understanding the data security lifecycle, enables the organization to map the different phases in the data lifecycle against the required controls that are relevant for each phase. The data lifecycle guidance provides a framework to map relevant use cases for data access, while assisting in the development and application of appropriate security controls within each lifecycle stage.

3.1. The Asset Lifecycle

To protect assets properly, one must understand the asset lifecycle and apply protection mechanism throughout the phases of the asset lifecycle. The protection will always be based on the value of those assets at particular points in that lifecycle. There are many other methodologies where there are more or less phases, or they might be named differently. Regardless, the point to be made here is that protection is required throughout the phases, and it is always based on the value of the assets at those particular moments in the lifecycle phases. The lifecycle includes six phases from creation to destruction. Although we show it as a linear progression, once created, data can bounce between phases without restriction, and may not pass through all stages (for example, not all data is eventually destroyed).

1. Create: This is probably better named Create/Update because it applies to creating or changing a data/content element, not just a document or database. Creation is the generation of new digital content, or the alteration/updating of existing content.
2. Store: Storing is the act committing the digital data to some sort of storage repository, and typically occurs nearly simultaneously with creation.
3. Use: Data is viewed, processed, or otherwise used in some sort of activity.
4. Share: Data is exchanged between users, customers, and partners.
5. Archive: Data leaves active use and enters long-term storage.

6. Destroy: Data is permanently destroyed using physical or digital means (e.g., cryptoshredding).

4. Classification and Categorization

Most dictionaries will define the words classification and categorization as follows. Classification is the act of forming into a class or classes. This can be rephrased as a distribution into groups, as classes, according to common attributes. Whereas categorization is the process of sorting or arranging things into classes. This can be simplified as saying classification is the system, and categorization is the act of sorting into the classification system.

4.1. Classification

The purpose of a classification system is to ensure protection of the assets based on value in such a way that only those with an appropriate level of clearance can have access to the assets. Many organizations will use the terms “confidential,” “proprietary,” or “sensitive” to mark assets. These markings may limit access to specific individuals, such as board members, or possibly certain sections of an organization, such as the human resources (HR) area or other key areas of the organization.

4.2. Categorization

Categorization is the process of determining the impact of the loss of confidentiality, integrity, or availability of the information to an organization. For example, public information on a web page may be low impact to an organization as it requires only minimal uptime, it does not matter if the information is changed, and it is globally viewable by the public. However, a startup company may have a design for a new clean power plant, which if it was lost or altered may cause the company to go bankrupt, as a competitor may be able to manufacture and implement the design faster. This type of information would be categorized as “high” impact. Classification and categorization is used to help standardize the protection baselines for information systems and the level of suitability and trust an employee may need to access information. By consolidating data of similar categorization and classification, organizations can realize economy of scale in implementing appropriate security controls. Security controls are then tailored for specific threats and vulnerabilities.

4.3. Data Classification and Policy

Data classification is all about analyzing the data that the organization has, in whatever form, determining its importance and value and then assigning it to a category or classification level. That category, or classification level, will determine the security requirements for protection of that valuable asset. For example, any data that is classified at the highest level, whether contained in a printed report or stored electronically, needs to be classified so that it can be handled and secured properly based on its classification. The requirements for classification should be outlined in a classification policy.

5. Data Classification Policy

- When classifying data, determine the following aspects of the policy:

Who will have access to the data: Define the roles of people who can access the data. Examples include accounting clerks who are allowed to see all accounts payable and receivable but cannot add new accounts and all employees who are allowed to see the names of other employees (along with managers' names and departments, and the names of vendors and contractors working for the company). However, only HR employees and managers can see the related pay grades, home addresses, and phone numbers of the entire staff. And only HR managers can see and update employee information classified as private, including Social Security numbers (SSNs) and insurance information.

- How the data is secured:

Determine whether the data is generally available or, by default, off limits. In other words, when defining the roles that are allowed to have access, you also need to define the type of access—view only or update capabilities—along with the general access policy for the data. As an example, many companies set access controls to deny database access to everyone except those who are specifically granted permission to view or update the data.

- How long the data is to be retained:

Many industries require that data be retained for a certain length of time. For example, many finance industries in countries may require specific retention periods. Data owners need to know the regulatory requirements for their data, and if requirements do not exist, they should base the retention period on the needs of the business.

- What method(s) should be used to dispose of the data:

For some data classifications, the method of disposal will not matter. But some data is so sensitive that data owners will want to dispose of printed reports through cross-cut shredding or another secure method. In addition, they may require employees to use a utility to verify that data has been removed fully from their PCs after they erase files containing sensitive data to address any possible data remanence issues or concerns.

- Whether the data needs to be encrypted:

Data owners will have to decide whether their data needs to be encrypted. They typically set this requirement when they must comply with a law or regulation such as the Payment Card Industry Data Security Standard (PCI DSS).

- The appropriate use of the data:

This aspect of the policy defines whether data is for use within the company, is restricted for use by only selected roles, or can be made public to anyone outside the organization. In addition, some data have associated legal usage definitions. The organization's policy should spell out any such restrictions or refer to the legal definitions as required. Proper data classification also helps the organization comply with pertinent laws and regulations. For example, classifying credit card data as private can help ensure compliance with the PCIDSS. One of the requirements of this standard is to encrypt credit card information. Data owners who correctly defined the encryption aspect of their organization's data classification policy will require that the data be encrypted according to the specifications defined in this standard.

6. Examples of Classification Levels

The requirement is that the definition of the classification levels should be clear enough so that it is easy to determine how to classify the data by the owners. Anyone else should also be able to easily understand how to protect the assets based on their classification levels. Also, it makes sense to use classification levels that truly reflect the value of the particular category.

Here are some examples of classification:

- Top Secret: Data that is defined as being very sensitive, possibly related to privacy, bank accounts, or credit card information.
- Company Restricted: Data that is restricted to properly authorized employees.
- Company Confidential: Data that can be viewed by many employees but is not for general use.
- Public: Data that can be viewed or used by employees or the general public.

What is important, however, is that whatever classifications are used, everyone in the organization must understand the value that each classification used represents, especially the owners who start the classification process and pass on the requirements to custodians and others.

6.1. Classification – Done by Owners

The individual who owns the data should decide the classification under which the data falls. We call that person the "owner." The data owner is best qualified to make this decision because he or she has the most knowledge about the use of the data and its value to the organization. Data owners should review their data's classification on a regular basis to ensure that the data remains correctly classified and protected based on that classification. As data moves through the data lifecycle, the owner is still in the best position to monitor value and ensure that the classification level reflects the data's true value. If any discrepancies are uncovered during the review, they need to be documented by the data owner and then reviewed with the proper individuals responsible for the data in question to establish the following:

- What caused the change in value, was it warranted and under what circumstances, and for what reason?
- Under whose authority was the change in classification carried out?
- What documentation, if any, exists to substantiate the change in value and, therefore, classification?

6.2. Purpose of Asset Classification

To summarize, the reason we classify assets, such as a data classification system, is to afford the assets the level of protection they require based on their value. The whole purpose of data classification is not only to express value but to protect based on the classification level. So, the value of data classification, is not only in the classification levels that are used but in the underlying mechanisms and architectures that provide the levels of protection required by each classification level. Careful implementation of technologies and support elements for data classification becomes very important. Support elements, such as education and training, become critical in allowing classification systems to work properly. In other words, classification is not only just having three or four classification categories, but having the careful implementation of effective supporting elements and security controls for each of the classification levels used.

As we have seen, data classification provides a way to protect assets based on value. This allows the organization to take care of some important and critical needs that can only be addressed through classification systems.

Some of these may include the following:

- Ensure that assets receive the appropriate level of protection based on the value of the asset.
- Provide security classifications that will indicate the need and priorities for security protection.
- Minimize risks of unauthorized information alteration.
- Avoid unauthorized disclosure.
- Maintain competitive edge.
- Protect legal tactics.
- Comply with privacy laws, regulations, and industry standards.

6.3. Classification Benefits

Other than the obvious benefit of protecting assets based on value, there are other potential benefits that can be realized by an organization in using asset classification systems. Here are some examples of these benefits:

- Awareness among employees and customers of the organization's commitment to protect information.
- Identification of critical information.
- Identification of vulnerability to modification.
- Enable focus on integrity controls.
- Sensitivity to the need to protect valuable information.
- Understanding the value of information.
- Meeting legal requirements.

6.4. Issues Related to Classification

Asset classification may have some other issues that the organization needs to address. The following may be examples of some of these issues, so in other words, these may include, and are not limited to:

- Human error.
- Proper classification is dependent on ability and knowledge of the classifier.
- Requires awareness of regulations and customer and business expectations.
- Requires consistent classification method—often the decisions can be somewhat arbitrary.
- Needs clear labeling of all classified items.
- Must include manner for declassifying and destroying material in classification process.

7. Asset Protection and Classification Terminology

In organizations, responsibilities for asset management, including data, have become increasingly divided among several roles. Asset management and data management need to include accountabilities and responsibilities for protection of assets based on classification. There are key roles that are identified in many laws and regulations that dictate certain accountabilities and responsibilities that organizations need to assign. This is especially true of privacy laws that exist

around the world, especially in very privacy-aware areas such as Europe. Laws for the protection of privacy have been enacted worldwide. Regardless of the jurisdiction, privacy laws tend to converge around the principle of allowing the individual to have control over their personal information, including how it is protected while it is being collected, processed, and stored by organizations. For organizations to protect the individual's personal information according to compliance requirements, they must assign accountability and responsibility properly. Compliance requirements will treat personal information as data that requires protection at every step of its lifecycle, from collection, to processing, to storage, to archiving, and to destruction.

Protection of data requires the clear distinction of roles, accountabilities, and responsibilities to be clearly identified and defined:

- **Data subject:** The individual who is the subject of personal data.
- **Data owner:** Accountable for determining the value of the data that they own and, therefore, also accountable for the protection of the data. Data owners also are accountable for defining policies for access of the data and clearly defining and communicating the responsibilities for such protection to other entities including stewards, custodians, and processors.
- **Data controller:** In the absence of a "true" owner, especially for personal information that has been collected by organizations belonging to clients and customers, the data controller is assigned the accountability for protecting the value of the information based on proper implementation of controls. The controller, either alone or jointly with others, determines the purposes for which and the manner in which any personal data is to be processed and, therefore, protected.
- **Data steward:** Data stewards are commonly responsible for data content, context, and associated business rules within the organization.
- **Data processor:** Data processors are the entities that process the data on behalf of the data controller, therefore, they may be given the responsibility to protect the data, although the accountability would always remain with the controller.
- **Data custodian:** Data custodians are responsible for the protection of the data while in their custody. That would mean safe custody, transport, storage, and processing of the data and the understanding and compliance to policies in regards to the protection of the data.

7.1. Data Ownership

Data management and protection involves many aspects of technology, but it also requires involved parties to clearly understand their roles and responsibilities. The objectives of delineating data management roles and responsibilities are to:

- Clearly define roles associated with functions.
- Establish data ownership throughout all phases of a project.
- Instill data accountability.
- Ensure that adequate, agreed-upon data quality and metadata metrics are maintained on a continuous basis.

7.2. Information Owner

When information is collected or created, someone in the organization needs to be clearly made accountable for it. We refer to this entity as the "owner." Often, this is the individual or group that created, purchased, or acquired the information to allow the organization to achieve its mission and goals. This individual or group is considered and referred to as the "information owner."

The information owner, therefore, is in the best position to clearly understand the value, either quantitative or qualitative, of the information. The owner is also accountable for protecting the information based on that value. To determine the correct value, the owner, therefore, has the following accountabilities:

- Determine the impact the information has on the mission of the organization.
- Understand the replacement cost of the information (if it can be replaced).
- Determine which laws and regulations, including privacy laws, may dictate liabilities and accountabilities related to the information.
- Determine who in the organization or outside of it has a need for the information and under what circumstances the information should be released.
- Know when the information is inaccurate or no longer needed and should be destroyed.

7.3. Documentation

It is very important for data owners to establish and document certain expectations that need to be passed on to others, such as custodians, as they relate to the data that is owned by the owners. For instance, these may be examples of documentation:

- The ownership, intellectual property rights, and copyright of their data.
- The obligations relevant to ensure the data is compliant with compliance requirements.
- The policies for protection of the data, including baselines and access controls.
- The expectations for protection and responsibilities delegated to custodians and others accessing the data.

7.4. Data Custodianship

Data custodians, as the word implies, have custody of assets that don't belong to them, usually for a certain period of time. Those assets belong to owners somewhere else, but the custodians have "custody" of those assets as they may be required for access, decisions, supporting goals, and objectives, etc. Custodians have the very important responsibility to protect the information while it's in their custody, according to expectations by the owners as set out in policies, standards, procedures, baselines, and guidelines. It will be up to the security function to ensure that the custodians are supported and advised and have the proper skills, tools, and architectures, etc. to be able to properly protect assets, such as information, while in their custody. How these aspects are addressed and managed should be in accordance with the defined data policies applicable to the data, as well as any other applicable data stewardship specifications. Typical responsibilities of a data custodian may include the following:

- Adherence to appropriate and relevant data policies, standards, procedures, baselines, and guidelines as set out by owners and supported by the security function.
- Ensuring accessibility to appropriate users, maintaining appropriate levels of data security.
- Fundamental data maintenance, including but not limited to data storage and archiving.
- Data documentation, including updates to documentation.
- Assurance of quality and validation of any additions to data, including supporting periodic audits to assure ongoing data integrity.

7.5. Difference Between Data Owner/Controller and Data Custodian/Processor

The difference between the data owner and the data custodian is that the owner is accountable for the protection of what they own based on the value of that asset to the organization. In an environment where a controller is required as part of compliance needs, the controller will act as the

owner and, therefore, becomes accountable for the protection based on expectations related to legislation and regulations and enforced through policy and the implementation of those policies as standards, procedures, baselines, and guidelines.

In other words:

Owners/Controllers:
Accountable for the protection of data based on relevant national or community laws or regulations. The natural or legal person, public authority, agency, or any other body that alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or community law.

Custodians/Processors:
The processor processes data on behalf of the owners (example cloud provider). Therefore, responsible for the adherence of policies, standards, procedures, baselines, and guidelines to ensure protection while in their custody.

8. Privacy

The global economy has, and still is, undergoing an information explosion. There has been massive growth in the complexity and volume of global information exchange and in general, information collection, processing, and storing. There is much more information and data that is available to everyone. Personal data is now very sensitive, and its protection and privacy have become important factors that organizations face as part of compliance requirements. The organization needs to protect the privacy of information as it is being collected, used, processed, stored, and archived by authorized individuals in the workplace. The following is an overview of some of the ways in which different countries and regions around the world are addressing the various legal and regulatory issues they face.

8.1. The United States

The United States has many sector-specific privacy and data security laws, both at the federal and state levels. There is no official national privacy data protection law or authority that governs privacy protection. In fact, privacy in the United States is said be a “sectorial” concern. For example, the Federal Trade Commission (FTC) has jurisdiction over most commercial entities and, therefore, has the authority to issue and enforce privacy regulations in specific areas. In addition to the FTC, there are other industry specific regulators, particularly those in the healthcare and financial services sectors, that have authority to issue and enforce privacy regulations. Generally, the processing of personal data is subject to “opt out” consent from the data subject, while the “opt in” rule applies in special cases such as the processing of sensitive and valuable health information. With regard to the accessibility of data stored within organizations, it is important to underline that the Fourth Amendment to the U.S. Constitution applies; it protects people from unreasonable searches and seizures by the government. The Fourth Amendment, however, is not a guarantee against all searches and seizures but only those that are deemed unreasonable under the law. Whether a particular type of search is considered reasonable in the eyes of the law is determined by balancing two important interests, the intrusion on an individual’s Fourth Amendment rights and the legitimate government interests such as public safety. In 2012, the US government unveiled a “Consumer Privacy Bill of Rights” as part of a comprehensive blueprint to protect individual privacy rights and

give users more control over how their information is handled by organizations that are collecting such information.

8.2. European Union

The data protection and privacy laws in the European Union (EU) member states are constrained by the EU directives, regulations, and decisions enacted by the EU. The main piece of legislation is the EU Directive 95/46/EC “on the protection of individuals with regard to the processing of personal data and on the free movement of such data.” These provisions apply in all business and, therefore, cover the processing of personal data in organizations. There is also the EU Directive 2002/58/EC (the ePrivacy Directive) “concerning the processing of personal data and the protection of privacy in the electronic communications sector.” This directive contains provisions that deal with data breaches and the use of cookies. Latin American, North Africa, and medium-size Asian countries have privacy and data protection legislation largely influenced by the EU privacy laws and, in fact, those EU privacy laws may have been used as models for specific legislation.

8.3. Asia–Pacific Economic Cooperation (APEC) Council

The Asia–Pacific Economic Cooperation (APEC) council has become the point of reference for the data protection and privacy regulations. The APEC countries have endorsed the APEC privacy framework, recognizing the importance of the development of effective privacy protections that avoid barriers to information flows and ensure continued trade and economic growth in the APEC region. The APEC privacy framework promotes a flexible approach to information privacy protection across APEC member economies, while avoiding the creation of unnecessary barriers to information flows.

8.4. Essential Requirements in Privacy and Data Protection Laws

The ultimate goal of privacy and data protection laws is to provide protection to individuals that are referred to as data subjects for the collection, storage, usage, and destruction of their personal data with respect to their privacy. This is achieved with the definitions of requirements to be fulfilled by the operators involved in the data processing. These operators can process the data, playing the role of data controllers or data processors; in other words, controllers end up having accountability for protection, and processors end up having responsibility for protection.

One such example is the Data Protection Act (DPA) in the UK. According to the Information Commissioner’s Office (ICO) of the UK, which is an independent organization devoted to uphold information rights in the public interest, promoting openness by public bodies and committed to data privacy for individuals, the Data Protection Act sets out rights for individuals regarding their personal information. Personal data is defined as information pertaining to an identifiable living individual. The DPA mandates that whenever personal data is processed, collected, recorded, stored or disposed of it must be done within the terms of the Data Protection Act (DPA). The Information Commissioner’s Office (ICO) helps organizations understand their compliance requirements and find out about their obligations and how to comply, including protecting personal information. As such they advise on how to comply with the DPA by providing any organization that handles personal information about individuals, a framework that guides how to meet the obligations under the DPA. The framework guides those who have day-to-day responsibility for data protection. It is split into eight data protection principles, and the guide explains the purpose and effect of each principle,

gives practical examples, and answers frequently asked questions. The data protection principles are as follows, taken directly from the ICO website:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless – (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

8.5. Organization for Economic Cooperation and Development (OECD) Guidelines on Privacy Protection

With the proliferation of technology and the increasing awareness that most of our personally identifiable information (PII) is stored online or electronically in some way and being collected, stored, and used by organizations, there is a need to protect personal information. That expectation today is in most cases dictated by privacy laws and regulations. There is an organization that has been devoted to helping governments and organizations around the world in dealing with issues that focus on improving the economic and social well-being of people around the world. That organizations is the OECD. The following is taken directly from the OECD website (www.oecd.org); it describes what the focus and initiatives of the OECD are. The OECD provides a forum in which governments can work together to share experiences and seek solutions to common problems. We work with governments to understand what drives economic, social, and environmental change. We measure productivity and global flows of trade and investment. We analyze and compare data to predict future trends. We set international standards on a wide range of things, from agriculture and tax to the safety of chemicals. We also look at issues that directly affect everyone's daily life, like how much people pay in taxes and social security and how much leisure time they can take. We compare how different countries' school systems are readying their young people for modern life and how different countries' pension systems will look after their citizens in old age. In the many decades that the OECD has existed, it has played an important role in promoting respect for privacy as a fundamental value and a condition for the free flow of personal data across borders. A perfect example of this is what the OECD has published as the 'OECD Privacy Guidelines.' These guidelines can act as a framework that organizations can use in order to understand and address the requirements of privacy protection. They can provide comprehensive guidance on what

organizations need to implement as far as security controls to address the requirements of the privacy principles.

8.5.1. OECD Privacy Guidelines

The OECD has broadly classified these principles into the collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.

The guidelines are as follows:

1. Collection Limitation Principle: There should be limits to the collection of personal data, and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. Data Quality Principle: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, and kept up-to-date.

3. Purpose Specification Principle: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. Use Limitation Principle: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified except with the consent of the data subject; or by the authority of law.

5. Security Safeguards Principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

6. Openness Principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. 7. Individual Participation Principle: An individual should have the right to a) obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; c) at a charge, if any, that is not excessive; d) in a reasonable manner; and in a form that is readily intelligible to him; e) to be given reasons if a request is denied, and to be able to challenge such denial; and f) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

8. Accountability Principle: A data controller should be accountable for complying with measures which give effect to the principles stated above.

9. Data Retention

Data retention, which is sometimes also referred to as records retention, is defined as the continued and long-term storage of valuable assets driven by compliance requirements or corporate requirements. Companies are required to comply with legal and regulatory legislation in retaining assets, especially information and records. Each company should have those requirements clearly addressed and expressed in a retention policy that usually is accompanied by a retention schedule. This will then provide the basis for how long to keep data and assets around and also when they should be securely destroyed.

9.1. Establishing Information Governance and Retention Policies

To understand retention requirements, we need to understand the various types of assets, such as data and records that may have retention needs. As part of proper asset governance, the establishment of effective asset archiving and retention policies needs to be done. These are the issues and factors to consider:

- Understand where the data exists: The enterprise cannot properly retain and archive data unless knowledge of where data resides and how different pieces of information relate to one another across the enterprise is available and known.

- Classify and define data: Define what data needs to be archived and for how long, based on business and retention needs that are driven by laws, regulations, and corporate requirements related to goals and objectives.

- Archive and manage data: Once data is defined and classified, the archiving of that data needs to be done appropriately, based on business access needs. Manage that archival data in a way that supports the defined data retention policies but at the same time allows authorized and timely access.

9.2. Examples of Data Retention Policies

Some examples of retention policies are as follows which you should all read via google.

1. European Document Retention Guide 2013: A Comparative View Across 15 Countries To Help You Better Understand Legal Requirements And Records Management Best Practices (Iron
1. Mountain, January 2013)
2. State of Florida Electronic Records and Records Management Practices, November 2010
3. The Employment Practices Code, Information Commissioner's Office, UK, November 2011
4. Wesleyan University, Information Technology Services Policy Regarding Data Retention for ITS-Owned Systems, September 2013
5. Visteon Corporation, International Data Protection Policy, April 2013
6. Texas State Records Retention Schedule (Revised 4th edition), effective July 4, 2012

10.Data Protection Methods

10.1. Baselines

A baseline is a minimum level of protection that can be used as a reference point. As a reference point, baselines can therefore be used as a comparison for assessments and requirements to ensure that those minimum levels of security controls are always being achieved. Baselines can also provide a way to ensure updates to technology and architectures are subjected to the minimum understood levels of security requirements. As part of what security does, once controls are in place to mitigate risks, the baselines can be referenced, after which all further comparisons and development are measured against it. Specifically when protecting assets, baselines can be particularly helpful in achieving protection of those assets based on value. Remember, if we have classified assets based on value, as long as we come up with meaningful baselines for each of the classification levels, we can conform to the minimum levels required. In other words, let's say that we are using classifications such as HIGH, MEDIUM, and LOW.

Baselines could be developed for each of our classifications and provide that minimum level of security required for each. For example, we could establish baselines as follows, keeping in mind that these examples may not be complete, they are just meant to show the concepts of how baselines can provide that reference point for minimum levels of security:

HIGH:

- Access
  - Strong passwords
  - Asset owner approved request, review, and termination process
  - Non-disclosure agreement
- Encryption
  - 128 bit symmetric encryption for creation, storage, and transmission
- Labelling
  - Watermark
- Monitoring
  - Real-time

MEDIUM:

- Access
  - passwords
  - Asset owner approved request, review, and termination process
- Encryption
  - 128 bit symmetric encryption for transmission
- Labeling
  - None
- Monitoring
  - Timely

LOW:

- Access
  - Asset owner approved request, review, and termination process
- Encryption
  - None

- Labelling
    - None
- Monitoring
    - None

Baselines can be technology and architecture related and specific to certain types of systems. For example, an organization may dictate what the minimum levels of security requirements need to be for a Windows machine before it can be connected to the corporate network. Baselines can also be non-technology related, such as an organization requiring all employees to display their identification badges while in certain areas of the organization, or requiring that any visitors must be escorted in valuable areas of the organizations. While these types of controls can be mandated and, therefore, be considered to be policies, they can also establish the minimum levels of security required as part of the security program and, therefore, create a baseline of protection.

As a summary:

1. A baseline is a consistent reference point.

2. Baselines provide a definition of the minimum level of protection that is required to protect valuable assets.

3. Baselines can be defined as configurations for various architectures, which will indicate the necessary settings and the level of protection that is required to protect that architecture.

In ISO 27001 and PCI DSS courses taught by AL Nafi we will cover in detail various baseline config guides and models.

In the mean time you can read the following to understand further how various configuration guides are created and updated based on best practices.

- United States Government Configuration Baseline (USGCB)
- Estonian Information System's Authority IT Baseline Security System ISKE

11.Generally Accepted Principles

This section introduces some generally accepted principles that address information security from a very high-level viewpoint that again can provide comprehensive guidance to organizations. These principles are fundamental in nature and rarely change over time, regardless of technology focus. They are NOT stated here as security requirements but are provided as useful guiding references for developing, implementing, and understanding security policies and baselines for use in any organization, regardless of industry or focus. The principles listed below are by no means exhaustive and only meant to be examples:

Information System Security Objectives: Information system security objectives or goals are described in terms of three overall objectives: confidentiality, integrity, and availability. Security policies, baselines, and measures are developed and implemented according to these objectives.

Prevent, Detect, Respond, and Recover: Information security is a combination of preventive, detective, response, and recovery measures. Preventive measures are for avoiding or deterring the

occurrence of an undesirable event. Detective measures are for identifying the occurrence of an undesirable event. Response measures refer to coordinated response to contain damage when an undesirable event (or incident) occurs. Recovery measures are for restoring the confidentiality, integrity, and availability of information systems to their expected state.

Protection of Information While Being Processed, in Transit, and in Storage: Security measures should be considered and implemented as appropriate to preserve the confidentiality, integrity, and availability of information while it is being processed, in transit, and in storage.

External Systems Are Assumed to Be Insecure: In general, an external system or entity that is not under your direct control should be considered insecure. Additional security measures are required when your information assets or information systems are located in, or interfacing with, external systems. Information systems infrastructure could be partitioned using either physical or logical means to segregate environments with different risk levels.

Resilience for Critical Information Systems: All critical information systems need to be resilient to withstand major disruptive events, with measures in place to detect disruption, minimize damage, and rapidly respond and recover.

Auditability and Accountability: Security requires auditability and accountability. Auditability refers to the ability to verify the activities in an information system. Evidence used for verification can take the form of audit trails, system logs, alarms, or other notifications. Accountability refers to the ability to audit the actions of all parties and processes that interact with information systems. Roles and responsibilities should be clearly defined, identified, and authorized at a level commensurate with the sensitivity of information.

12.Scoping and Tailoring

Scoping can be defined as limiting the general baseline recommendations by removing those that do not apply. We “scope” to ensure the baseline control applies to the environment as best as it can. Tailoring is defined as altering baseline control recommendations to apply more specifically. This means we “tailor” to make sure controls apply as required probably specifically to the technology or environment. To scope and tailor, a thorough understanding of the environment and risks is necessary.

Scoping guidance provides an enterprise with specific terms and conditions on the applicability and implementation of individual security controls. Several considerations can potentially impact how baseline security controls are applied by the enterprise. System security plans should clearly identify which security controls employed scoping guidance and include a description of the type of considerations that were made. The application of scoping guidance must be reviewed and approved by the authorizing official for the information system in question.

Tailoring involves scoping the assessment procedures to more closely match the characteristics of the information system and its environment of operation. The tailoring process gives enterprises the flexibility needed to avoid assessment approaches that are unnecessarily complex or costly while simultaneously meeting the assessment requirements established by applying the fundamental concepts of a risk management framework. Supplementation involves adding assessment procedures or assessment details to adequately meet the risk management needs of the organization (e.g., adding organization-specific details such as system/platform-specific information for selected security controls). Supplementation decisions are left to the discretion of the organization to

maximize flexibility in developing security assessment plans when applying the results of risk assessments in determining the extent, rigor, and level of intensity of the assessments.
Be aware of the value that scoping, tailoring, and supplementation can bring to the security architectures being planned and assessed for the enterprise. The use of scoping and tailoring to properly narrow the focus of the architecture will ensure that the appropriate risks are identified and addressed based on requirements. The use of supplementation will allow the architecture to stay flexible over time and grow to address the needs of the enterprise that arise during operation of the architecture once it is implemented fully and as time goes on.

Various frameworks which are outside of the scope of exams, but Al Nafi we will be covering those frameworks in a separate class before the final exam.

13. The Center for Strategic & International Studies (CSIS) 20 Critical Security Controls Initiative

The need to understand the scope of the security needs to be addressed, as well as the business requirements to be supported and the resources available to accomplish the tasks at hand are all part of the formula for success that you must learn to master. The Center for Strategic & International Studies (CSIS) 20 Critical Security Controls initiative provides a unified list of 20 critical controls that have been identified through a consensus of federal and private industry security professionals as the most critical security issues seen in the industry. The CSIS team includes officials from the NSA, US Cert, DoD JTF-GNO, the Department of Energy Nuclear Laboratories, Department of State, DoD Cyber Crime Center, and the commercial sector. The CSIS controls do not introduce any new security requirements, but they organize the requirements into a simplified list to aid in determining compliance and ensure that the most important areas of concern are addressed.
In 2013, the stewardship and sustainment of the Controls was transferred to the Council on Cyber Security (the Council), an independent, global, non-profit entity committed to a secure and open internet. The CSIS initiative is designed to help the federal government prioritize resources and consolidate efforts to reduce costs and ensure that the critical security issues are addressed. The five "critical tenets" of the CSIS initiative, as listed on the SANS website, are as follows:

Offense Informs Defense: Use knowledge of actual attacks that have compromised systems to provide the foundation to build effective, practical defenses. Include only those controls that can be shown to stop known real-world attacks.

Prioritization: Invest first in controls that will provide the greatest risk reduction and protection against the most dangerous threat actors and that can be feasibly implemented in your computing environment.

Metrics: Establish common metrics to provide a shared language for executives, IT specialists, auditors, and security officials to measure the effectiveness of security measures within an organization so that required adjustments can be identified and implemented quickly.

Continuous Monitoring: Carry out continuous monitoring to test and validate the effectiveness of current security measures.

Automation: Automate defenses so that organizations can achieve reliable, scalable, and continuous measurements of their adherence to the controls and related metrics.

13.1. Current List of Critical Security Controls – Version 5.1

The current list of Critical Security Controls—Version 5.1 are as follows:

- Inventory of Authorized and Unauthorized Devices
- Inventory of Authorized and Unauthorized Software
- Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- Continuous Vulnerability Assessment and Remediation
- Malware Defenses
- Application Software Security
- Wireless Access Control
- Data Recovery Capability
- Security Skills Assessment and Appropriate Training to Fill Gaps
- Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- Limitation and Control of Network Ports, Protocols, and Services
- Controlled Use of Administrative Privileges
- Boundary Defense
- Maintenance, Monitoring, and Analysis of Audit Logs
- Controlled Access Based on the Need to Know
- Account Monitoring and Control
- Data Protection
- Incident Response and Management
- Secure Network Engineering
- Penetration Tests and Red Team Exercises

14.Data States

It is typically agreed upon that data and information can be in three basic states: data at rest, data in motion (transit), and data in use. Understanding these three states and how information and data can be represented in each of the states can allow an organization to apply the security measures that are appropriate for its protection.

1. Data at Rest: data stored on media in any type of form. It is at rest because it is not being transmitted or processed in any way.

2. Data in Motion: data that is currently traveling, typically across a network. It is in motion because it is moving.

3. Data in Use: data that is being processed by applications or processes. It is in use because it is data that is currently in the process of being generated, updated, appended, or erased. It might also be in the process of being viewed by users accessing it through various endpoints or applications.

14.1. Data at Rest

The protection of stored data is often a key requirement for a company's sensitive information. Databases, backup information, off-site storage, password files, and many other types of sensitive information need to be protected from disclosure or undetected alteration and availability. Much of

this can be done through the use of cryptographic algorithms that limit access to the data to those that hold the proper encryption (and decryption) keys. Some modern cryptographic tools also permit the condensing, or compressing, of messages, saving both transmission and storage space, making them very efficient.

Data at Rest – Description of Risk
Malicious users may gain unauthorized physical or logical access to a device, transfer information from the device to an attacker's system, and perform other actions that jeopardize the confidentiality of the information on a device.

Data at Rest – Recommendations
Removable media and mobile devices must be properly encrypted, following the guidelines below when used to store valuable data. Mobile devices include laptops, tablets, wearable tech, and smartphones. Proper access controls and redundancy controls also need to be applied to protect data at rest.

14.2. Data in Transit

Data that moves, usually across networks, is said to be data in motion, or in transit. One of the primary needs of organizations today is to move data and information across various types of media, but the need is to prevent the contents of the message from being revealed even if the message itself was intercepted in transit. Whether the message is sent manually, over a voice network, or via the internet, or any other network, including wireless networks, modern cryptography can provide secure and confidential methods to transmit data and allows the verification of the integrity of the message so that any changes to the message itself can be detected. Recent advances in quantum cryptography have shown that the "viewing" of a message can be detected while in transit.

14.2.1. Link Encryption

Data are encrypted on a network using either link or end-to-end encryption. In general, link encryption is performed by service providers, such as a data communications provider on a Frame Relay network. Link encryption encrypts all of the data along a communications path (e.g., a satellite link, telephone circuit, or T-1 line). Because link encryption also encrypts routing data, communications nodes need to decrypt the data to continue routing. The data packet is decrypted and re-encrypted at each point in the communications channel. It is theoretically possible that an attacker compromising a node in the network may see the message in the clear. Because link encryption also encrypts the routing information, it provides traffic confidentiality better than end-to-end encryption. Traffic confidentiality hides the addressing information from an observer, preventing an inference attack based on the existence of traffic between two parties.

14.2.2. End-to-End Encryption

End-to-end encryption is generally performed by the end user within an organization. The data are encrypted at the start of the communications channel or before and remain encrypted until decrypted at the remote end. Although data remain encrypted when passed through a network, routing information remains visible. An example of end-to-end encryption would be a virtual private network (VPN) connection.

14.3. Data in Transit – Description of Risk

The risks associated with data in motion are the same as those associated with data at rest. These include unauthorized disclosure, modification, and unavailability. Malicious actors may intercept or monitor plaintext data transmitting across network and gain unauthorized access that jeopardizes the confidentiality, integrity, and availability of the data.

Data in Transit will be discussed further in PCI DSS and ISO 27001 courses taught by Al Nafi along with its uses cases and real life implementations.

15.Media Handling

15.1. Media

Media storing sensitive information requires physical and logical controls. Media lacks the means for digital accountability when the data is not encrypted. For this reason, extensive security must be taken when handling sensitive media. Logical and physical controls, such as marking, handling, storing, and declassification, provide methods for the secure handling of sensitive media containing sensitive information.

15.2. Marking

Organizations should have policies in place regarding the marking and labeling of media based on its classification. For example:

Storage media should have a physical label identifying the sensitivity of the information contained. The label should clearly indicate if the media is encrypted. The label may also contain information regarding a point of contact and a retention period. When media is found or discovered without a label, it should be immediately labeled at the highest level of sensitivity until the appropriate analysis reveals otherwise.

The need for media marking typically is strongest in organizations where sensitive intellectual property and confidential data must be stored and shared among multiple people. If the security architect can design centrally managed and controlled enterprise content management (ECM) systems paired with Data Loss (Leakage) Protection technology (DLP), then the entire threat vector that media marking is designed to address may be able to be handled in a totally different way as well.

15.3. Handling

Only designated personnel should have access to sensitive media. Policies and procedures describing the proper handling of sensitive media should be promulgated. Individuals responsible for managing sensitive media should be trained on the policies and procedures regarding the proper handling and marking of sensitive media. Never assume that all members of the organization are fully aware of or understand security policies. It is also important that logs and other records be used to track the activities of individuals handling backup media. Manual processes, such as access logs, are necessary to compensate for the lack of automated controls regarding access to sensitive media.

15.4. Storing

Sensitive media should not be left lying about where a passerby could access it. Whenever possible, backup media should be encrypted and stored in a security container, such as a safe or strong box with limited access. Storing encrypted backup media at an off-site location should be considered for disaster recovery purposes. Sensitive backup media stored at the same site as the system should be kept in a fire-resistant box whenever possible.

In every case, the number of individuals with access to media should be strictly limited, and the separation of duties and job rotation concepts should be implemented where it is cost effective to do so.

15.5. Destruction

Media that is no longer needed or is defective should be destroyed rather than simply disposed of. A record of the destruction should be used that corresponds to any logs used for handling media. Implement object reuse controls for any media in question when the sensitivity is unknown rather than simply recycling it.

15.6. Record Retention

Information and data should be kept only as long as it is required. Organizations may have to keep certain records for a period as specified by industry standards or in accordance with laws and regulations. Hard- and soft-copy records should not be kept beyond their required or useful life. Security practitioners should ensure that accurate records are maintained by the organization regarding the location and types of records stored. A periodic review of retained records is necessary to reduce the volume of information stored and ensure that only relevant information is preserved.

Record retention policies are used to indicate how long an organization must maintain information and assets. Ensure the following:

- The organization understands the retention requirements for different types of data throughout the organization.
- The organization documents in a record's schedule the retention requirements for each type of information.
- The systems, processes, and individuals of the organization retain information in accordance with the schedule but not longer.

A common mistake in records retention is finding the longest retention period and applying it without analysis to all types of information in an organization. This not only wastes storage but also adds considerable "noise" when searching or processing information in search of relevant records. Records and information no longer mandated to be retained should be destroyed in accordance with the policies of the enterprise and any appropriate legal requirements that may need to be taken into account.

16.Data Remanence

Data remanence is defined as the residual data remaining on some sort of object after the data has been deleted or erased. The problem related to data remanence is that there may some physical characteristics of that data remaining on the media even after we've tried to securely erase it.

Depending on the value of the data, it may be very important to securely erase the data so that there are no residual characteristics remaining that may allow anyone to recover the information. On a typical hard disk drive (HDD), the data is represented onto the hard drive by using magnetic technology. In other words, the zeroes and the ones are represented by using magnetic technology. This type of technology can be used to re-record new data onto the drive as we can alter the magnetic field so that we can overwrite and erase any data that may have been represented onto the data previously.

Solid-state drive (SSD) technology, which is newer technology, does not use magnetic fields to represent the information, instead, it uses flash memory to store data. Flash technology uses electrons that change the electronic “charge” in a “flash” to represent the information. That is why it is called “flash” technology. Flash memory, such as SSD, does not require power as moving parts are not required to access any stored data.

Data remaining on media that use magnetic technologies, such as HDDs, become an issue if the value of the data that was stored on that media is high. Since there may be methods to recover the original data, sanitizing the information must be done effectively by using secure methods. Secure methods to address data remanence (data remaining on the media after erasure) can be summarized by three options. These options are clearing, purging, and destruction.

16.1. Clearing

Clearing is defined as the removal of sensitive data from storage devices, using methods that provide some assurance that the data may not be reconstructed using most known data recovery techniques. The original data may still be recoverable but typically not without special recovery techniques and skills.

16.2. Purging

Purging, sometimes referred to as sanitizing, is the removal of sensitive data from media with the intent that the sensitive data cannot be reconstructed by any known technique.

16.3. Destruction

This is exactly as it sounds. The media is made unusable by using some sort of destruction method. This could include shredding, or melting the media into liquid by using very high temperatures. We must note, however, that the effectiveness of destroying the media varies. For example, simply drilling a hole through a hard drive may allow most of the data to still be recovered, whereas, melting the hard drive into liquid would not. The destruction method should be driven by the value of the sensitive data that is residing on the media. To summarize, destruction using appropriate techniques is the most secure method of preventing retrieval. Destruction of the media is the best method as it destroys the media and also the data that is on it. However, the destruction method must be a very good one to prevent the recovery of the data. If we ensure that the data cannot be reconstructed, we refer to that as defensible destruction of the data. In other words, we ensure that the data is not recoverable.

16.4. Data Destruction Methods

As we have discussed, the three options available to address data remanence are clearing, purging, and destruction. Destruction is thought of as being the best option, as long as the destruction method is a good one. The following methods may fit into the three categories as described above:

Overwriting: One common method used to address data remanence is to overwrite the storage media with new data. We can overwrite with zeroes or ones. This is sometimes called wiping. The simplest overwrite technique is to write zeroes over the existing data, and depending on the sensitivity of the data, this might need to be done several times.

Degaussing: During the mainframe days, a technology called degaussing was created. This technique uses a degausser that basically erases the information on the magnetic media by applying a varying magnetic field to the media to erase the information that was stored using magnetic technology. The media is basically saturated with a magnetic field that erases all of the information. Since this uses a magnetic field to saturate the media, it can be useful for any technology that uses magnetic technology to represent the data, including mainframe tapes and also HDDs. While many types of older magnetic storage media, such as tapes, can be safely degaussed, degaussing usually renders the magnetic media of modern HDDs completely unusable, which may be ultimately desirable to address remanence properly.

Encryption: Encrypting data before it is stored on the media can address data remanence very effectively. But this is only true if the encryption key used to encrypt the information is then destroyed securely. This would make it very difficult, if not impossible, for an untrusted party to recover any data from the media. The industry refers to this process as crypto-erase or in some cases, crypto-shredding. This method of addressing data remanence may be very useful in cloud environments.

16.5. Media Destruction – Defensible Destruction

As we have discussed, destruction of the media and the data on it is the most desirable way to address data remanence. But this is only effective based on the method used for destruction. Defensible destruction implies that the method used will not allow the reconstruction and recovery of that data contained on the media device itself through any known means. The following may be examples of effective defensible destruction methods:

- Physically breaking the media apart, such as hard drive shredding, etc.
- Chemically altering the media into a non-readable state by possibly using corrosive chemicals.
- Phase transition, which means using temperature and pressure to change the state of something into something else.
- For media using magnetic technology, raising its temperature above the Curie Temperature, which is at the point where devices lose their magnetic properties.

16.6. Solid-State Drives (SSDs)

Solid-State Drives (SSDs) use flash memory for data storage and retrieval. Flash memory differs from magnetic memory in one key way: flash memory cannot be overwritten. When existing data on an HDD is changed, the drive overwrites the old data with the new data. This makes overwriting an

effective way of erasing data on an HDD. However, when changes are made to existing data on an SSD, the drive writes that data, along with the new changes, to a different location rather than overwriting the same section. The flash translation layer then updates the map so that the system finds the new, updated data rather than the old data. Because of this, an SSD can contain multiple iterations of the same data, even if those iterations are not accessible by conventional means. This is what causes data remanence on SSDs.

16.6.1. Solid-State Drive (SSD) Data Destruction

SSDs have a unique set of challenges that require a specialized set of data destruction techniques. Unlike HDDs, overwriting is not effective for SSDs. Because the flash translation layer controls how the system is able to access the data, it can effectively "hide" data from data destruction software, leaving iterations of the data un-erased on different sections of the drive. Instead, SSD manufacturers include built-in sanitization commands that are designed to internally erase the data on the drive. The benefit of this is that the flash translation layer does not interfere with the erasure process. However, if these commands were improperly implemented by the manufacturer, this erasure technique will not be effective.

Another technique, called cryptographic erasure or crypto-erase, takes advantage of the SSD's built-in data encryption. Most SSDs encrypt data by default. By erasing the encryption key, the data will then be unreadable. However, this approach relies again on being able to effectively erase data despite interference by the flash translation layer. If the flash translation layer masks the presence of any data pertaining to the encryption, the "encrypted" drive may still be readable.
Due to the unique complexities of SSDs, the best data destruction method is, in fact, a combination of techniques such as crypto-erase, sanitization, and overwrite. SSDs require the careful data destruction techniques to effectively prevent data remanence on SSDs. The use of cloud-based storage today also presents a data remanence challenge for the organizations moving to the cloud. As more and more data is being moved to the cloud, the ability to address data security issues in general can become much more difficult for the enterprise.

16.7. Cloud-Based Data Remanence

Among the many challenges that face the security practitioner in this area is the ability to authoritatively certify that data has been successfully destroyed upon decommissioning of cloud-based storage systems. Due to the fact that a third party owns and operates the system and the enterprise is effectively renting storage space, there is little to no visibility into the management and security of the data in many cases. While the challenge is a big one for the enterprise, the use of Platform as a Service-based (PaaS) architectures can actually provide a solution for the issues raised by data remanence in the cloud. The security practitioner and the cloud vendor have to be willing to work together to architect a PaaS solution that addresses the daunting issues of media and application-level encryption via a platform offering. There are many parts that have to be properly set up and synchronized for this solution to work, such as messaging, data transactions, data storage and caching, and framework APIs. In addition, the platform has to be set up in such a way, with appropriate safeguards available, to ensure that no unencrypted data is ever written to physical media at any time during the data lifecycle, including data in transit.

